

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-276188  
 (43)Date of publication of application : 30.09.1994

(51)Int.Cl. H04L 9/00  
 H04L 9/10  
 H04L 9/12  
 G06F 13/00  
 H04L 9/06  
 H04L 9/14  
 H04L 12/22

(21)Application number : 05-060794 (71)Applicant : TOSHIBA CORP  
 (22)Date of filing : 22.03.1993 (72)Inventor : OTA TETSUO

## (54) ELECTRONIC COMMUNICATION EQUIPMENT

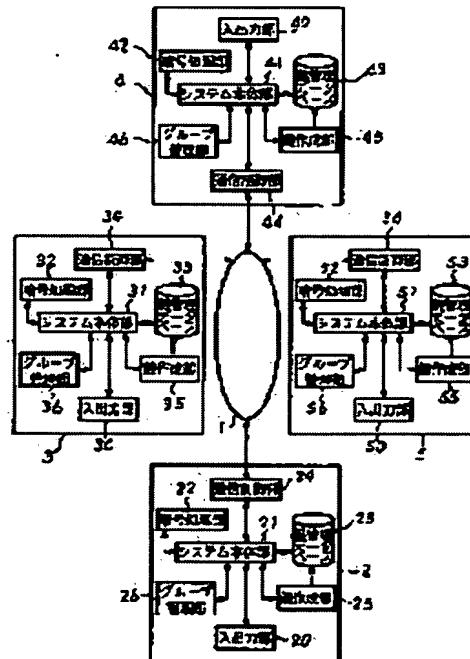
### (57)Abstract:

**PURPOSE:** To improve a processing speed and safety at the time of performing security holding communication by providing a cipher processing part for performing an enciphering processing and a deciphering processing for executing the instruction of a system main body part and a key preparation part for preparing a common key.

**CONSTITUTION:** This electronic communication equipment connects plural computer systems 2-5 through a communication medium 1. In the electronic communication equipment operated on the computer network, the system main body parts 21, 31, 41 and 51 instruct the mutual identification of users, the distribution of the common key and the

transmission/reception of communication information using the common key. Also, the cipher processing parts 22, 32, 42 and 52 for performing the enciphering processing and the deciphering processing for mutually identifying the users, distributing the common key and transmitting/receiving the communication information

using the common key and the key preparation parts 25, 35, 45 and 55 for preparing the common key are provided. Thus, it is guaranteed that the communication information is originated from the correct user, the communication information can be deciphered only by the correct user and efficient mutual identification and safe communication can be performed. Thus, the processing speed and the safety at the time of the security holding communication can be improved.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-276188

(43)公開日 平成6年(1994)9月30日

(51)Int.Cl. <sup>5</sup> H 0 4 L 9/00 9/10 9/12	識別記号 8949-5K 8949-5K	府内整理番号 F I	技術表示箇所 Z Z
審査請求 未請求 請求項の数3 O L (全13頁) 最終頁に続く			

(21)出願番号 特願平5-60794

(22)出願日 平成5年(1993)3月22日

(71)出願人 000003078  
株式会社東芝  
神奈川県川崎市幸区堀川町72番地  
(72)発明者 太田 哲生  
神奈川県川崎市幸区柳町70番地 株式会社  
東芝柳町工場内  
(74)代理人 弁理士 則近 憲佑

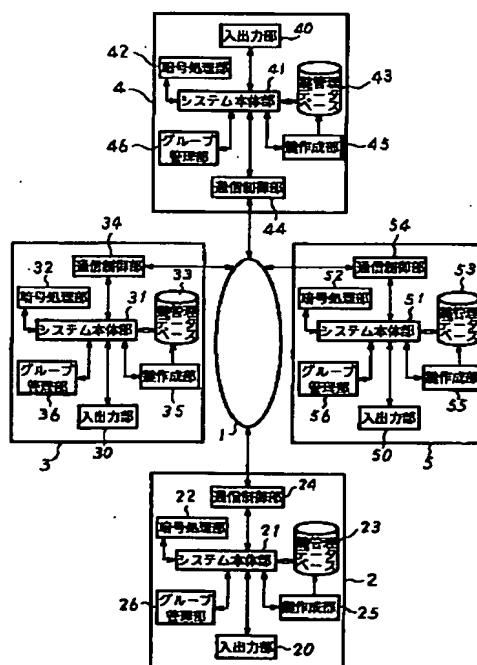
(54)【発明の名称】 電子通信装置

(57)【要約】

【目的】 機密保持通信を行う際の、処理速度と安全性の向上を目的とする。

【構成】 本発明は、コンピュータネットワーク上で動作する電子通信装置において、利用者相互の認証、共通鍵の配布、前記共通鍵を用い通信情報の送受信を命令するシステム本体部と、利用者相互の認証、共通鍵の配布、前記共通鍵を用い通信情報の送受信を行うために暗号化処理と復号化処理を行う暗号処理部と、前記共通鍵を作成する鍵作成部とを具備する。

【効果】 通信情報が正しい利用者から発信されたことを保証し、同通信情報が正しい利用者のみに解読でき、効率のよい相互認証と安全な通信が可能になる。



## 【特許請求の範囲】

【請求項1】複数のコンピュータシステムが通信媒体により相互に接続されたコンピュータネットワーク間で暗号化した通信情報の送受信を行う電子通信装置において、

- ( a ) 公開鍵暗号方式を用い利用者相互の認証
- ( b ) 公開鍵暗号方式を用い共通鍵の配布
- ( c ) 前記共通鍵を用い通信情報の送受信

を命令するシステム本体部と、  
前記システム本体部の命令を実行するための暗号化処理部と復号化処理を行う暗号処理部と、

前記共通鍵を作成する鍵作成部とを具備する電子通信装置。

【請求項2】一定時間及び一定通信回数ごとに利用者の一部が前記共通鍵を更新することのできる鍵作成トークンを持つ前記鍵作成部と、

前記利用者の一部が通信を中止するとき、他の利用者に鍵作成トークンの使用を命令するシステム本体部とを具備する請求項1記載の電子通信装置。

【請求項3】サブグループ間の機密保持通信を行うために、サブグループ間に有効な共通鍵を作成する前記鍵作成部を具備する請求項1記載の電子通信装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、複数のコンピュータシステムが通信媒体により相互に接続されたコンピュータネットワーク上で、機密を保持する機能をもつ電子通信装置に関する。

## 【0002】

【従来の技術】機密保持を行う通信は、通信以前にコンピュータシステムを使用する利用者が正しい利用者であるかを確認すること（以下、認証と呼ぶ。）がまず重要である。

【0003】従来、通常の秘密保持通信と通常の秘密通信を行ふ前の認証を考慮した通信装置として、以下に示す慣用暗号方式を用いた第1の電子通信装置と第2の電子通信装置と、公開鍵暗号方式を用いた第3の電子通信装置があつた。

【0004】慣用暗号方式による2つの電子通信装置は、以下に示す2つの暗号化の方法の組み合わせによって構成される。第1の暗号化の方法は、あらかじめ通信情報の暗号化と暗号化された通信情報の復号を行うための一つの鍵を作成し、この鍵をそれぞれ利用者のコンピュータシステムに配布し、配布されたこの鍵を持つ利用者のコンピュータシステムのみ通信可能とする暗号化の方法である。

【0005】第2の暗号化の方法は、それぞれの利用者のコンピュータシステムが通信する特定のコンピュータシステム間にのみ有効な鍵を持ち、通信相手ごとに異なるこの鍵を用いて、受信人毎に異なる暗号化した情報を

作成し通信を行うための暗号化の方法である。

【0006】この第2の暗号化の方法でn人の利用者が暗号化通信する場合、鍵は全部で $n(n-1)/2$ 個必要であった。例えば、利用者 $\alpha$ と利用者 $\beta$ が通信するときの鍵を $[\alpha: \beta]$ とする。（ここで、 $[\alpha: \beta]$ と $[\beta: \alpha]$ は同じ鍵であるとする。）5人の利用者 $\alpha$ 、利用者 $\beta$ 、利用者 $\gamma$ 、利用者 $\delta$ 、利用者 $\epsilon$ が通信するとき、鍵は全部で $[\alpha: \beta]$ 、 $[\alpha: \gamma]$ 、 $[\alpha: \delta]$ 、 $[\alpha: \epsilon]$ 、 $[\beta: \gamma]$ 、 $[\beta: \delta]$ 、 $[\beta: \epsilon]$ 、 $[\gamma: \delta]$ 、 $[\gamma: \epsilon]$ 、 $[\delta: \epsilon]$ と10個必要であった。

【0007】従来の慣用暗号方式を用いた第1の電子通信装置は、利用者同士の認証と他のコンピュータシステム利用者への通信情報の送信を上述の慣用暗号方式の第2の暗号化の方法で暗号化通信を行うことを特徴とした装置であり、第2の電子通信装置は、利用者同士の認証を慣用暗号方式の第2の暗号化の方法で行い、他のコンピュータシステム利用者への通信情報の送信を慣用暗号方式の第1の暗号化の方法で行うことを特徴とした装置であった。

【0008】公開暗号方式を用いた第3の電子通信装置について以下、「利用者 $\alpha$ が利用者 $\beta$ に情報を送信し、利用者 $\beta$ が利用者 $\alpha$ からのこの情報を受信する」という通信を例に説明する。

【0009】利用者は、それぞれ自分のみが持つ秘密鍵と自分以外の利用者の公開された公開鍵を持つ。この秘密鍵と公開鍵は、（イ）利用者 $\alpha$ の公開鍵で暗号化された情報は、利用者 $\alpha$ の秘密鍵で復号する、（ロ）利用者 $\alpha$ の秘密鍵で暗号化された情報は、利用者 $\alpha$ の公開鍵で復号する、という対応関係をもつている。

【0010】この対応関係を利用して、利用者 $\alpha$ のコンピュータシステムは、利用者 $\beta$ の公開鍵で情報を暗号化し、さらにこの利用者 $\beta$ の公開鍵で暗号化した情報を、利用者 $\alpha$ の秘密鍵で暗号化し送信する。

【0011】利用者 $\beta$ のコンピュータシステムは、受信した情報を利用者 $\alpha$ の公開鍵で復号し、さらにこの利用者 $\alpha$ の公開鍵で復号した情報を利用者 $\beta$ の秘密鍵で復号する。

【0012】このような手順で、情報をやりとりする方法が公開暗号方式を用いた電子通信装置である。これを以下第3の電子通信装置と呼ぶ。この公開暗号方式を用いた電子通信装置は、n人の利用者が通信するためには自分の秘密鍵と自分以外の利用者の公開鍵を用い、電子通信装置全体で $2n$ 個の鍵を用いる。

## 【0013】

【発明が解決しようとする課題】上述したような第1の電子通信装置で認証と通信する場合および第2の電子通信装置で認証する場合は、n人の利用者の認証をする場合、装置全体で $n(n-1)/2$ 個という大量の鍵が必要で、鍵の配布だけでも時間がかかり、また、鍵を記憶

させるだけで多くの記憶領域や作業領域を使用してしまい、高速で効率のよい通信が不可能であるという問題点があった。更に、鍵の漏洩については特に対策がなされておらず、通信情報の安全性についての問題点と、1つの情報の送信を行う利用者が  $n(n-1)/2$  個の鍵を用いて受信者ごとに送信する通信情報が異なるためネットワーク上の同報機能が使用できず、個別に送信しなければならないという問題点があった。

【 0014 】第2の電子通信装置で通信する場合、通信情報の暗号化と暗号化された通信情報の復号を行うための一つの鍵を使用するが、この装置も鍵が漏洩してしまうと機密を保持した通信が不可能であると言う問題点があった。

【 0015 】第3の電子通信装置は、1つの情報の送信を行う利用者がそれぞれの受信者の公開鍵を用いて受信者の数だけ暗号化通信を行う必要があるため、時間がかかり、受信者ごとに送信する通信情報の内容が異なるためネットワーク上の同報機能が使用できず、個別に送信しなければならないという問題点があった。また、長時間同一の鍵を使用する場合、鍵の漏洩の可能性もあり、通信情報の安全性についても問題点があった。

【 0016 】

【 課題を解決するための手段】本発明は、複数のコンピュータシステムが通信媒体により相互に接続されたコンピュータネットワーク間で暗号化した通信情報の送受信を行う電子通信装置において、

- ( a ) 公開鍵暗号方式を用い利用者相互の認証
- ( b ) 公開鍵暗号方式を用い共通鍵の配布
- ( c ) 前記共通鍵を用い通信情報の送受信

を命令するシステム本体部と、前記システム本体部の命令を実行するための暗号化処理と復号化処理を行う暗号処理部と、前記共通鍵を作成する鍵作成部とを具備することを特徴とする。

【 0017 】また、一定時間及び一定通信回数ごとに利用者の一部が前記共通鍵を更新することのできる鍵作成トークンを持つ前記鍵作成部と、前記利用者の一部が通信を中止するとき、他の利用者に鍵作成トークンの使用を命令するシステム本体部とを具備することを特徴とする。さらに、サブグループ間の機密保持通信を行うために、サブグループ間に有効な共通鍵を作成する前記鍵作成部を具備することを特徴とする。

【 0018 】

【 作用】上記構成の電子通信装置によれば、あらかじめに公開鍵を利用者に配布し、通信情報を送信する利用者の秘密鍵を用いて公開暗号方式で暗号化することにより、この通信情報が前記送信する利用者か送信したことを保証し、さらにこの通信情報を受信する利用者の公開鍵を用いて暗号化することにより、この通信情報が受信人のみに解読でき、従来の装置にくらべ認証の際送信する通信情報が少なく相互認証を効率よく行うことができ

る。

【 0019 】利用者は、相互認証後利用者間で、その後の通信の暗号に用いる共通鍵を共通鍵作成手段において作成し、前記公開暗号方式で配布することにより、安全に共通鍵を配布することができ、さらに定期的に更新することにより、通信の安全性を高めることができる。

【 0020 】利用者が送信する通信情報は、送信を行う利用者の秘密鍵と前記公開暗号方式で配布された共通鍵の双方を用いて機密保持暗号化を行い、送信する通信情報が受信する利用者に関係なく同一のものとなり、同報機能の使用が可能になる。

【 0021 】安全性向上のため、定期的に共通鍵の更新を行うが、利用者が勝手に更新を行うと共通鍵の一貫性を保持することができないため、鍵作成のプログラムの実行権である鍵作成トークンを使用可能な利用者に鍵の作成を委任することにより、共通鍵の一貫性を保持することが可能となる。

【 0022 】鍵作成トークンを他の利用者に使用可能にすることにより、利用者は自由に通信に加入あるいは中止することが可能になる。利用者の一部でさらに機密保持通信を行うためのサブグループを作成する場合、複数の鍵作成トークンを用いてサブグループごとに異なった共通鍵を利用することにより、サブグループ内の通信においても機密保持が可能となる。

【 0023 】

【 実施例】以下、本発明の一実施例を図面を基に説明する。図1は本発明の一実施例の構成図である。ここではまず、図1を用いて利用者Aと利用者Bが認証しあう手順を簡単に説明する。

【 0024 】本電子通信装置は、通信媒体1を介して、複数のコンピュータシステム2、3、4、5が接続されている。利用者Aは、コンピュータシステム2の入出力部20に、利用者が利用者Aであることを示す利用者Aのパスワードを入力する。

【 0025 】入出力部20は、入力された利用者が利用者Aであることを示す利用者Aのパスワードをシステム本体部21に送る。システム本体部21は、入力された利用者が利用者Aであることを示す利用者Aのパスワードを暗号処理部22に送る。

【 0026 】システム本体部21は、あらかじめ鍵管理データベース23に登録されている利用者Bの公開鍵と利用者Aの秘密鍵を暗号処理部22に送り、暗号化を命令する。

【 0027 】暗号処理部22は、利用者Bの公開鍵を用いて、利用者Aのパスワードを暗号化する。暗号処理部22は、利用者Aの秘密鍵を用い暗号化されたパスワードをさらに暗号化する。

【 0028 】暗号処理部22は、さらに暗号化された利用者Aのパスワードをシステム本体部21に送る。システム本体部21は、このさらに暗号化された利用者Aの

5

パスワードを通信制御部24に送り、コンピュータシステム3への送信を命令する。

【0029】通信制御部24は、さらに暗号化された利用者Aのパスワード302を通信媒体1を介してコンピュータシステム3の通信制御部34に送る。通信制御部34は、通信媒体1を介し通信制御部24が送信したさらに暗号化された利用者Aのパスワード302を受信する。

【0030】通信制御部34は、さらに暗号化された利用者Aのパスワードをシステム本体部31に送る。システム本体部31は、このさらに暗号化された利用者Aのパスワードを暗号処理部32に送る。

【0031】システム本体部31は、鍵管理データベース33に登録されている利用者Aの公開鍵と利用者Bの秘密鍵を暗号処理部22に送り、復号化を命令する。暗号処理部32は、利用者Aの公開鍵で、さらに暗号化された利用者Aのパスワードを復号する。ここでは、さらに暗号化された利用者Aのパスワードは、復号化された利用者Aのパスワードになる。

【0032】暗号処理部32は、復号化された利用者Aのパスワードをシステム本体部31に送る。システム本体部31は、正しく復号できたかを判断する。

【0033】システム本体部31は、復号できなかつた場合、本装置を終了させる。システム本体部31は、正しく復号できた場合、暗号処理部32に復号化を命令する。

【0034】暗号処理部32は、利用者Bの秘密鍵で、復号化された利用者Aのパスワードを復号する。暗号処理部32は、さらに復号化された利用者Aのパスワードをシステム本体部31に送る。

【0035】システム本体部31は、正しく復号できたかを判断する。システム本体部31は、復号できなかつた場合、本装置を終了させる。なお、正しく復号できた場合、このさらに復号化された利用者Aのパスワードは、利用者Aのパスワードと同じものである。

【0036】システム本体部31は、正しく復号できた場合、さらに復号化された利用者Aのパスワードを入出力部30に送る。入出力部30は、さらに復号化された利用者Aのパスワード、つまり、利用者Aのパスワードを出力する。

【0037】利用者Bは、入出力部30にさらに復号化された利用者Aのパスワード、つまり、利用者Aのパスワードが出力されたことにより、送信者が利用者Aであることを認証する。

【0038】この後、逆に利用者Bから利用者Aに同様の手続きで送信することにより、利用者Aと利用者Bの相互の認証を行う。以下、上述の利用者Aと利用者Bの認証の手順を図2のフローチャートと図3の通信情報の形式を示す図を基に詳しく説明する。

【0039】利用者Aは、図2に示す「Aのパスワード

6

を入力」200のステップで、図1のコンピュータシステム2の入出力部20に、図3に示す利用者が利用者Aであることを示す利用者Aのパスワード300を入力する。

【0040】入出力部20は、入力された利用者が利用者Aであることを示す利用者Aのパスワード300をシステム本体部21に送る。システム本体部21は、入力された利用者が利用者Aであることを示す利用者Aのパスワード300を暗号処理部22に送る。

【0041】システム本体部21は、あらかじめされている鍵管理データベース23に登録されている利用者Bの公開鍵と利用者Aの秘密鍵を暗号処理部22に送り、暗号化を命令する。

【0042】暗号処理部22は、ステップ「Bの公開鍵で暗号化」201にあるように、利用者Bの公開鍵を用いて、利用者Aのパスワード300を暗号化する。ここでは、利用者Aのパスワード300は、暗号化された利用者Aのパスワード301になる。

【0043】暗号処理部22は、ステップ「Aの秘密鍵で暗号化」202にあるように、利用者Aの秘密鍵を用いて、暗号化された利用者Aのパスワード301を暗号化する。ここでは、暗号化された利用者Aのパスワード301は、さらに暗号化された利用者Aのパスワード302になる。

【0044】暗号処理部22は、さらに暗号化された利用者Aのパスワード302をシステム本体部21に送る。システム本体部21は、このさらに暗号化された利用者Aのパスワード302を通信制御部24に送り、コンピュータシステム3への送信を命令する。

【0045】通信制御部24は、ステップ「暗号化されたパスワードの送信」203にあるように、さらに暗号化された利用者Aのパスワード302を通信媒体1を介してコンピュータシステム3の通信制御部34に送る。

【0046】通信制御部34は、ステップ「暗号化されたパスワードの受信」204にあるように、通信媒体1を介し通信制御部24が送信したさらに暗号化された利用者Aのパスワード302を受信する。

【0047】通信制御部34は、さらに暗号化された利用者Aのパスワード302をシステム本体部31に送る。システム本体部31は、このさらに暗号化された利用者Aのパスワード302を暗号処理部32に送る。

【0048】システム本体部31は、鍵管理データベース33に登録されている利用者Aの公開鍵と利用者Bの秘密鍵を暗号処理部22に送り、復号化を命令する。暗号処理部32は、ステップ「Aの公開鍵で復号化」205にあるように、利用者Aの公開鍵で、さらに暗号化された利用者Aのパスワード302を復号する。ここでは、さらに暗号化された利用者Aのパスワード302は、復号化された利用者Aのパスワード303になる。

【0049】暗号処理部32は、復号化された利用者A

のパスワード303をシステム本体部31に送る。システム本体部31は、ステップ「復号できた?」206にあるように正しく復号できたかを判断する。

【0050】システム本体部31は、復号できなかった場合、ステップ「エラー終了」207にあるように、本装置を終了させる。なお、正しく復号できた場合、この復号化された利用者Aのパスワード303は、暗号化された利用者Aのパスワード301と同じものになる。

【0051】システム本体部31は、正しく復号できた場合、暗号処理部32に復号化を命令する。暗号処理部32は、ステップ「Bの秘密鍵で復号化」208にあるように、利用者Bの秘密鍵で、復号化された利用者Aのパスワード303を復号する。ここでは、復号化された利用者Aのパスワード303は、さらに復号化された利用者Aのパスワード304になる。

【0052】暗号処理部32は、さらに復号化された利用者Aのパスワード304をシステム本体部31に送る。システム本体部31は、ステップ「復号できた?」209にあるように、正しく復号できたかを判断する。

【0053】システム本体部31は、復号できなかった場合、ステップ「エラー終了」207にあるように、本装置を終了させる。なお、正しく復号できた場合、このさらに復号化された利用者Aのパスワード304は、利用者Aのパスワード300と同じものになる。

【0054】システム本体部31は、正しく復号できた場合、さらに復号化された利用者Aのパスワード304、つまり、利用者Aのパスワード300を入出力部30に送る。

【0055】入出力部30は、ステップ「Aのパスワードの出力」210にあるように、さらに復号化された利用者Aのパスワード304、つまり、利用者Aのパスワード300を出力する。

【0056】利用者Bは、入出力部30にさらに復号化された利用者Aのパスワード304、つまり、利用者Aのパスワード300が送出されたことにより、送信者が利用者Aであることを認証する。

【0057】利用者全員が暗号化処理のためにもつ共通鍵を配布する手順は、共通鍵を持つ利用者あるいは、共通鍵を作成した利用者が、上述のパスワードを送信する手順で、パスワードではなく共通鍵を通信情報として送信することにより配布する。

【0058】また、パスワードと共通鍵を同時に送信することにより、認証と共通鍵の配布が一度に行うことができる。本電子通信装置の機密保持暗号化通信の手順を、図1の構成図を基に簡単に説明する。

【0059】利用者Aは、入出力部20に利用者Aの通信情報を入力する。入出力部20は、利用者Aの通信情報をシステム本体部21に送る。システム本体部21は、利用者Aの通信情報を暗号処理部22に送る。

【0060】システム本体部21は、鍵管理データベー

ス23に登録されている利用者Aの秘密鍵と共通鍵を暗号処理部22に送り、暗号化を命令する。暗号処理部22は、利用者Aの通信情報を利用者Aの秘密鍵を用いて暗号化する。

【0061】暗号処理部22は、暗号化された利用者Aの通信情報を鍵管理データベース23に登録されている共通鍵を用いてさらに暗号化する。暗号処理部22は、さらに暗号化された利用者Aの通信情報をシステム本体部21に送る。

【0062】システム本体部21は、さらに暗号化された利用者Aの通信情報を通信制御部24に送り、コンピュータシステム3、4、5に送信を命令する。通信制御部24は、通信媒体1を介して、さらに暗号化された利用者Aの通信情報を利用者B、利用者C、利用者Dのコンピュータシステム3、4、5の通信制御部34、44、54に送信する。

【0063】コンピュータシステム3、4、5の通信制御部34、44、54は、さらに暗号化された利用者Aの通信情報を受信する。通信制御部34、44、54は、さらに暗号化された利用者Aの通信情報を本体システム部31、41、51に送る。

【0064】本体システム部31、41、51は、さらに暗号化された利用者Aの通信情報を暗号処理部32、42、52に送る。本体システム部31、41、51は、鍵管理データベース33、43、53に登録されている共通鍵と利用者Aの公開鍵を暗号処理部32、42、52に送り、復号化を命令する。

【0065】暗号処理部32、42、52は、さらに暗号化された利用者Aの通信情報を、共通鍵で復号する。

【0066】暗号処理部32、42、52は、復号化された利用者Aの通信情報を本体システム部31、41、51に送る。

【0067】本体システム部31、41、51は、正しく復号できたかを判断する。本体システム部31、41、51は、復号できなかった場合は、本装置を終了させる。

【0068】本体システム部31、41、51は、復号化された利用者Aの通信情報の復号化を暗号処理部32、42、52に命令する。暗号処理部32、42、52は、利用者Aの公開鍵で復号化された利用者Aの通信情報を復号する。

【0069】暗号処理部32、42、52は、このさらに復号化された利用者Aの通信情報を本体システム部31、41、51に送る。本体システム部31、41、51は、正しく復号できたかを判断する。本体システム部31、41、51は、復号できなかった場合は、本装置を終了させる。

【0070】本体システム部31、41、51は、正しく復号できた場合、このさらに復号化された利用者Aの通信情報、つまり、利用者Aの通信情報を入出力部30、40、50に送り、出力を命令する。

【 0 0 7 0 】 入出力部3 0 、 4 0 、 5 0 は、さらに復号化された利用者Aの通信情報、つまり、利用者Aの通信情報を出力する。以下、上述した通信情報の機密保持暗号化通信を具体的に、図4のフローチャートと図5の通信情報の形式を示す図を基に説明する。

【 0 0 7 1 】 利用者Aは、図4のステップ「Aの通信情報入力」4 0 0 にあるように、図1の入出力部2 0 に図5に示す利用者Aの通信情報5 0 0 を入力する。入出力部2 0 は、利用者Aの通信情報5 0 0 をシステム本体部2 1 に送る。

【 0 0 7 2 】 システム本体部2 1 は、利用者Aの通信情報5 0 0 を暗号処理部2 2 に送る。システム本体部2 1 は、鍵管理データベース2 3 に登録されている利用者Aの秘密鍵と共通鍵を暗号処理部2 2 に送り、暗号化を命令する。

【 0 0 7 3 】 暗号処理部2 2 は、ステップ「Aの秘密鍵で暗号化」4 0 1 にあるように、利用者Aの通信情報5 0 0 を利用者Aの秘密鍵を用いて暗号化する。ここでは、利用者Aの通信情報5 0 0 は、暗号化された利用者Aの通信情報5 0 1 になる。

【 0 0 7 4 】 なお、この暗号化は秘密鍵を有する真の利用者しか行えないため、通信情報に署名を行うことと同様の効果がある。暗号処理部2 2 は、ステップ「共通鍵で暗号化」4 0 2 にあるように、暗号化された利用者Aの通信情報5 0 1 を、鍵管理データベース2 3 に登録されている共通鍵を用いて暗号化する。ここでは、暗号化された利用者Aの通信情報5 0 1 は、さらに暗号化された利用者Aの通信情報5 0 2 になる。

【 0 0 7 5 】 暗号処理部2 2 は、さらに暗号化された利用者Aの通信情報5 0 2 をシステム本体部2 1 に送る。システム本体部2 1 は、さらに暗号化された利用者Aの通信情報5 0 2 を通信制御部2 4 に送り、コンピュータシステム3 、 4 、 5 に送信を命令する。

【 0 0 7 6 】 通信制御部2 4 は、ステップ「通信情報の送信」4 0 3 にあるように、通信媒体1 を介して、さらに暗号化された利用者Aの通信情報5 0 2 を利用者B、利用者C、利用者Dのコンピュータシステム3 、 4 、 5 の通信制御部3 4 、 4 4 、 5 4 に送信する。

【 0 0 7 7 】 コンピュータシステム3 、 4 、 5 の通信制御部3 4 、 4 4 、 5 4 は、ステップ「通信情報の受信」4 0 4 にあるように、さらに暗号化された利用者Aの通信情報5 0 2 を受信する。

【 0 0 7 8 】 通信制御部3 4 、 4 4 、 5 4 は、さらに暗号化された利用者Aの通信情報5 0 2 を本体システム部3 1 、 4 1 、 5 1 に送る。本体システム部3 1 、 4 1 、 5 1 は、さらに暗号化された利用者Aの通信情報5 0 2 を暗号処理部3 2 、 4 2 、 5 2 に送る。

【 0 0 7 9 】 本体システム部3 1 、 4 1 、 5 1 は、鍵管理データベース3 3 、 4 3 、 5 3 に登録されている共通鍵と利用者Aの公開鍵を暗号処理部3 2 、 4 2 、 5 2 に

送り、復号化を命令する。

【 0 0 8 0 】 暗号処理部3 2 、 4 2 、 5 2 は、ステップ「共通鍵で復号化」4 0 5 にあるように、さらに暗号化された利用者Aの通信情報5 0 2 を、共通鍵で復号する。ここでは、さらに暗号化された利用者Aの通信情報5 0 2 は、復号化された利用者Aの通信情報5 0 3 になる。

【 0 0 8 1 】 暗号処理部3 2 、 4 2 、 5 2 は、復号化された利用者Aの通信情報5 0 3 を本体システム部3 1 、 4 1 、 5 1 に送る。本体システム部3 1 、 4 1 、 5 1 は、ステップ「復号できた？」4 0 6 にあるように、正しく復号できたかを判断する。

【 0 0 8 2 】 本体システム部3 1 、 4 1 、 5 1 は、復号できなかった場合は、ステップ「エラー終了」4 0 7 にあるように、本装置を終了させる。なお、正しく復号できた場合、この復号化された利用者Aの通信情報5 0 3 は、暗号化された利用者Aの通信情報5 0 1 と同じものになる。

【 0 0 8 3 】 本体システム部3 1 、 4 1 、 5 1 は、復号化された利用者Aの通信情報5 0 3 の復号化を暗号処理部3 2 、 4 2 、 5 2 に命令する。暗号処理部3 2 、 4 2 、 5 2 は、ステップ「Aの公開鍵で復号化」4 0 8 にあるように、利用者Aの公開鍵で復号化された利用者Aの通信情報5 0 3 を復号する。ここでは、復号化された利用者Aの通信情報5 0 3 は、さらに復号化された利用者Aの通信情報5 0 4 になる。

【 0 0 8 4 】 暗号処理部3 2 、 4 2 、 5 2 は、このさらに復号化された利用者Aの通信情報5 0 4 を本体システム部3 1 、 4 1 、 5 1 に送る。本体システム部3 1 、 4 1 、 5 1 は、ステップ「復号できた？」4 0 9 にあるように、正しく復号できたかを判断する。本体システム部3 1 、 4 1 、 5 1 は、復号できなかった場合は、ステップ「エラー終了」4 0 7 にあるように、本装置を終了させる。

【 0 0 8 5 】 なお、正しく復号できた場合、このさらに復号化された利用者Aの通信情報5 0 4 は、利用者Aの通信情報5 0 0 と同じものになる。本体システム部3 1 、 4 1 、 5 1 は、正しく復号できた場合、このさらに復号化された利用者Aの通信情報5 0 4 、つまり、利用者Aの通信情報5 0 0 を入出力部3 0 、 4 0 、 5 0 に送り、出力を命令する。

【 0 0 8 6 】 入出力部3 0 、 4 0 、 5 0 は、ステップ「通信情報の出力」4 1 0 にあるように、さらに復号化された利用者Aの通信情報5 0 4 、つまり、利用者Aの通信情報5 0 0 を出力する。

【 0 0 8 7 】 安全性を確保するため、共通鍵を更新する例を図6のフローチャートを基に説明する。共通鍵の更新は、上述した機密保持暗号化通信において、鍵管理データベース2 3 に登録されている共通鍵を用いて暗号化するとき(図4のフローチャートのステップ「共通鍵で

11

暗号化」402の処理)に行う。ここでは、利用者Aが鍵作成部に共通鍵を作成するプログラムの実行権である共通鍵作成トーケンを持ち、利用者Aが一定回数ごとに通信を行うと、共通鍵を更新作成するものとする。

【0088】本体システム部21は、ステップ「共通鍵作成トーケンの有無?」600にあるように鍵作成部25に共通鍵作成トーケンがあるか否か判断する。共通鍵作成トーケンが無い場合、つまり、利用者A以外の利用者が共通鍵を用いて通信情報を暗号化する場合、ステップ「今までの共通鍵で暗号化」601にあるように、本体システム部21は、現在使われている共通鍵での暗号化を命令(上述の図4のフローチャートのステップ「共通鍵で暗号化」402の処理)し、機密保持暗号化通信を行う。

【0089】共通鍵作成トーケンを持つ場合、つまり、利用者Aが共通鍵を用いて通信情報を暗号化する場合、本体システム部21は、ステップ「カウンタを+1」602にあるように、鍵管理データベース23にあるカウンタを更新する。

【0090】本体システム部21は、ステップ「カウンタが設定値以上?」603にあるように、カウンタが設定値以上かどうか判断する。カウンタが、設定値未満の場合、ステップ「今までの共通鍵で暗号化」601にあるように、本体システム部21は、現在使われている共通鍵での暗号化を命令(上述の図4のフローチャートのステップ「共通鍵で暗号化」402の処理)し、機密保持暗号化通信を行う。

【0091】設定値に達した場合、本体システム部21は、ステップ「共通鍵を作成」604にあるように、新しい共通鍵を作成することを鍵作成部25に命令する。鍵作成部25は、新しい共通鍵を作成し、ステップ「共通鍵を登録」605にあるように、鍵管理データベース23に登録する。

【0092】本体システム部21は、ステップ「カウンタを0」606にあるように、鍵管理データベース23のカウンタを0にする。本体システム部21は、鍵管理データベース23に登録した新しい共通鍵を暗号処理部22に送り、暗号化の処理を命令する。

【0093】暗号処理部22は、上述の認証の手順つまり、共通鍵配布の手順で暗号化の処理をし、本体システム部21に送る。本体システム部21は、この暗号化の処理をされた共通鍵を通信制御部24に送る。

【0094】通信制御部24は、ステップ「共通鍵の配布」607にあるように、上述の認証の手順つまり、共通鍵配布の手順で他の利用者全員に配布する。利用者A、B、C、Dのコンピュータシステム2、3、4、5は、ステップ「新しい共通鍵で暗号化」608にあるように、この新しい共通鍵で通信情報を暗号化(上述の図4のフローチャートの「共通鍵で暗号化」402の処理)し、機密保持暗号化通信を行う。

12

【0095】このように定期的に共通鍵を更新することにより、万が一、共通鍵が漏洩した場合でも通信の安全性を保持することができる。共通鍵作成トーケンを持つ利用者が、他の利用者に共通鍵作成トーケンを移す共通鍵作成トーケンの委譲処理について説明する。

【0096】通常の通信において、共通鍵作成トーケンの委譲は共通鍵の一貫性の保持と、一定回数ごとの共通鍵の更新ということを考慮すると避けるべきことである。しかし、共通鍵作成トーケンを持つ者が通信を中止する場合、一定回数及び一定時間ごとの共通鍵の更新ができなくなるため、他のメンバに対して共通鍵作成トーケンを委譲する必要がある。

【0097】委譲処理は、上述の認証の手順、つまり、共通鍵配布の手順と同様の通信手順で、共通鍵作成トーケンの委譲の命令を通信情報として送信することで行う。具体的に、図7のフローチャートを基に、利用者Aが通信を中止し、利用者Aが共通鍵作成トーケンを持つ場合には共通鍵作成トーケンをBに委譲処理する手順を説明する。

20 【0098】利用者Aは、ステップ「通信中止コマンド入力」700にあるように、入出力部21に通信を中止するコマンドを入力する。入出力部21は、暗号処理部22に通信中止の命令を送る。

【0099】暗号処理部22は、ステップ「共通鍵作成トーケンの有無?」701にあるように、鍵管理データベース23に共通鍵作成トーケンがあるか否かを判断する。共通鍵作成トーケンが無い場合、暗号処理部22は、通信制御部24に通信を中止し、通信媒体1との接続を解除する命令を送る。

30 【0100】通信制御部24は、ステップ「接続解除」702にあるように、コンピュータシステム2と通信媒体1との接続を解除する。共通鍵作成トーケンがある場合、暗号処理部22は、入出力部21に共通鍵作成トーケンを委譲する利用者名の入力を促す提示を行わせる。

【0101】利用者Aは、ステップ「委譲する利用者名の入力」703にあるように、どの利用者に共通鍵作成トーケンを委譲するかの入力を入出力部21に行う。入出力部21は、共通鍵作成トーケンの委譲の命令を暗号処理部22に送る。

40 【0102】暗号処理部22は、通信制御部24に共通鍵作成トーケンの委譲の命令を送る。通信制御部24は、ステップ「共通鍵作成トーケンの委譲命令の送信」704にあるように、上述の認証の手順、つまり、共通鍵配布の手順と同様の通信手順で、共通鍵作成トーケンの委譲の命令を利用者Bのコンピュータシステム3の通信制御部34に送信する。

【0103】通信制御部34は、ステップ「共通鍵作成トーケンの委譲命令の受信」705にあるように、利用者Aの共通鍵作成トーケンの委譲命令を受信し、暗号処理部32に送る。

【 0104 】 暗号処理部3 2 は、ステップ「 共通鍵作成トーケンの登録」 706 にあるように、利用者A の共通鍵作成トーケンの委譲命令を解読し、今後共通鍵作成トーケンを持つことを鍵管理データベース3 3 に登録する。

【 0105 】 暗号処理部3 2 は、共通鍵作成トーケンの登録が完了したことを通信制御部3 4 に送る。通信制御部3 4 は、ステップ「 登録完了メッセージの送信」 707 にあるように、共通鍵作成トーケンの登録が完了したことを見たメッセージを利用者A のコンピュータシステム2 の通信制御部2 4 に送信する。

【 0106 】 通信制御部2 4 は、ステップ「 登録完了メッセージの受信」 708 にあるように、共通鍵作成トーケンの登録が完了したことを示すメッセージを受信。通信制御部2 4 は、暗号処理部2 2 に共通鍵作成トーケンの登録が完了したことを示すメッセージを送る。

【 0107 】 暗号処理部2 2 は、共通鍵作成トーケンの登録が完了したことを示すメッセージを解読し、通信を中止し、通信媒体1 との接続を解除する命令を通信制御部2 4 に送る。

【 0108 】 通信制御部2 4 は、ステップ「 接続解除」 702 にあるように、コンピュータシステム2 と通信媒体1 との接続を解除する。このように、共通鍵作成トーケンの委譲により、通信の自由な参加、退席が可能になる。

【 0109 】 通信中に利用者の一部分で、さらに機密保持通信を行いたい場合のサブグループ作成の手順について、図8 のフローチャートと図9 のサブグループを管理するためのグループ管理情報群の構造を示す図を基に説明する。ここでは、グループ名、利用者情報リスト、鍵作成トーケンの有無、共通鍵、カウンタという横一列がひとつのグループ管理情報である。

【 0110 】 利用者A は、図8 に示すステップ「 グループ情報入力」 800 にあるように、入出力部2 1 にサブグループの名称であるグループ名、利用者名や利用者のアドレス、共通鍵作成トーケンの有無の入力を行う。ここでは、入出力部2 1 は、グループ管理部2 6 に入力されたグループ名、利用者情報( メンバ名、アドレス) 、共通鍵作成トーケンの有無をグループ管理部2 6 に送る。

【 0111 】 グループ管理部2 6 は、ステップ「 グループ情報登録」 801 にあるように、図9 に示すグループ管理情報9 0 に、グループ名をグループ名9 0 0 のように登録し、利用者情報を利用者情報リスト9 0 1 、9 0 2 、9 0 3 のように登録し、共通鍵作成トーケンの有無を共通鍵作成トーケンの有無9 0 4 のように登録する。ここでは、「 有」 と登録する。

【 0112 】 グループ管理部2 6 は、鍵作成部2 5 に共通鍵の作成を命令する。鍵作成部2 5 は、ステップ「 共通鍵の作成」 802 にあるように、サブグループ内の共

通鍵を作成する。

【 0113 】 鍵作成部2 5 は、作成したサブグループ内の共通鍵をグループ管理部2 6 に送る。グループ管理部2 6 は、ステップ「 共通鍵の登録」 803 にあるように、グループ管理情報9 0 に、サブグループ内の共通鍵をサブグループ共通鍵9 0 5 のように、グループ管理情報9 0 に登録する。

【 0114 】 グループ管理部2 6 は、ステップ「 カウンタを0」 804 にあるように、サブグループ内の共通鍵の更新のため、サブグループ内の共通鍵の使用回数を数えるためのグループ通信カウンタ9 0 6 を0 にセットする。

【 0115 】 グループ管理部2 6 は、グループ管理情報9 0 の共通鍵作成トーケンの有無9 0 4 を「 無」としたグループ管理情報を暗号処理部2 2 に送る。暗号処理部2 2 は、サブグループの利用者のみに、ステップ「 グループ情報の配布」 805 にあるように、前記グループ管理情報を上述の認証の手順つまり、共通鍵配布と同様の手順で配布する。

【 0116 】 配布された前記グループ管理情報のサブグループ共通鍵を利用することにより、前記グループ情報管理を持つサブグループの利用者間のみで、秘密情報通信が可能となる。

【 0117 】

【 発明の効果】 本発明の電子通信装置によれば、相互認証の際、利用者はあらかじめ配布された公開鍵を持ち、通信情報を送信する利用者の秘密鍵を用いて公開暗号化方式で暗号化することにより、前記通信情報が前記利用者から送信されたことを保証し、さらに前記通信情報を受信人の公開鍵を用いて暗号化することにより、通信情報が受信人のみに解読でき、従来の装置にくらべ認証の際送信する通信情報が少なく相互認証を効率よく行うことができる。

【 0118 】 鍵作成トーケンを持つ利用者が共通鍵を作成し、上述の公開暗号方式で配布することにより、安全に共通鍵を配布することができ、さらに定期的に更新することにより、通信の安全性を高めることができる。

【 0119 】 また、複数の利用者の通信において、発信人の秘密鍵と公開暗号方式で配布された共通鍵の双方を用いて暗号化を行った場合、同一の通信情報の送信で共通鍵を持つ利用者のみ受信が可能である。

【 図面の簡単な説明】

【 図1】 本発明の一実施例の構成を示す図。

【 図2】 本発明の一実施例における利用者の認証の手順を示す図。

【 図3】 本発明の一実施例における利用者の認証の際に暗号化された通信情報の形式と復号化された通信情報の形式を示す図。

【 図4】 本発明の一実施例における機密暗号化通信の手順を示す図。

【図5】本発明の一実施例における機密暗号化通信の際に暗号化された通信情報の形式と復号化された通信情報の形式を示す図。

【図6】本発明の一実施例における共通鍵の更新の手順を示す図。

【図7】本発明の一実施例における共通鍵作成トーケンの委譲処理の手順を示す図。

【図8】本発明の一実施例におけるサブグループの作成の手順を示す図。

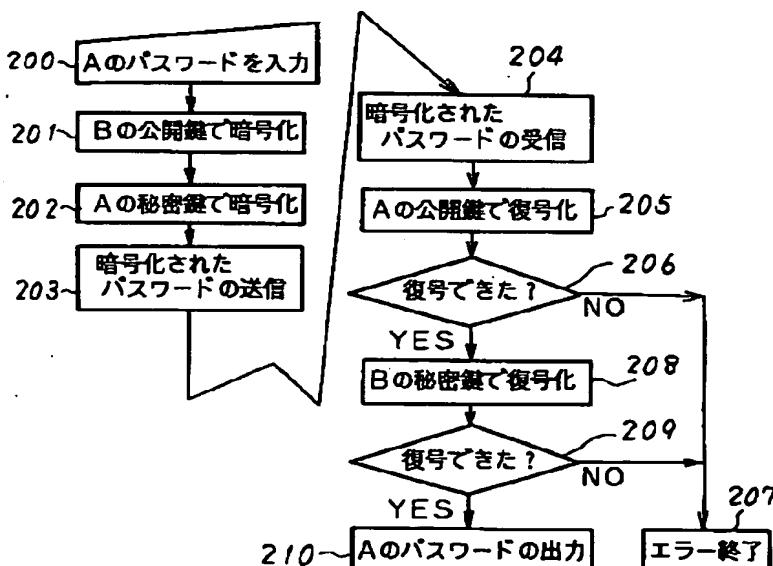
【図9】本発明の一実施例におけるサブグループ作成の際のグループ管理情報群の構造を示す図。

【符号の説明】

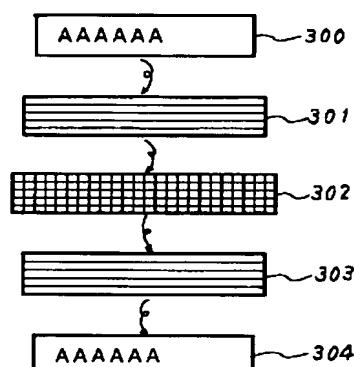
- 1 通信媒体
- 2、3、4、5 コンピュータシステム
- 20、30、40、50 入出力部
- 21、31、41、51 本体システム部
- 22、32、42、52 暗号処理部
- 23、33、43、53 鍵管理データベース
- 24、34、44、54 通信制御部
- 25、35、45、55 鍵作成部
- 26、36、46、56 グループ管理部

- 300 利用者Aが入力した通信情報
- 301 利用者Bの公開鍵で暗号化されたパスワードの形式
- 302 利用者Aの秘密鍵で暗号化されたパスワードの形式
- 303 利用者Aの公開鍵で復号化されたパスワードの形式
- 304 利用者Bの秘密鍵で復号化されたパスワードの形式
- 500 利用者Aが入力した通信情報の形式
- 501 利用者Aの秘密鍵で暗号化された通信情報の形式
- 502 共通鍵で暗号化された通信情報の形式
- 503 共通鍵で復号化された通信情報の形式
- 504 Aの公開鍵で復号化された通信情報の形式
- 90 グループ管理情報
- 900 グループ名
- 901、902、903 利用者情報リスト
- 904 鍵作成トーケンの有無
- 20 905 サブグループ共通鍵
- 906 グループ通信カウンタ

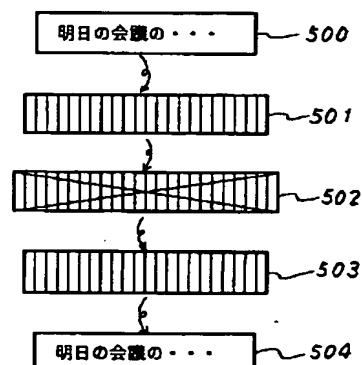
【図2】



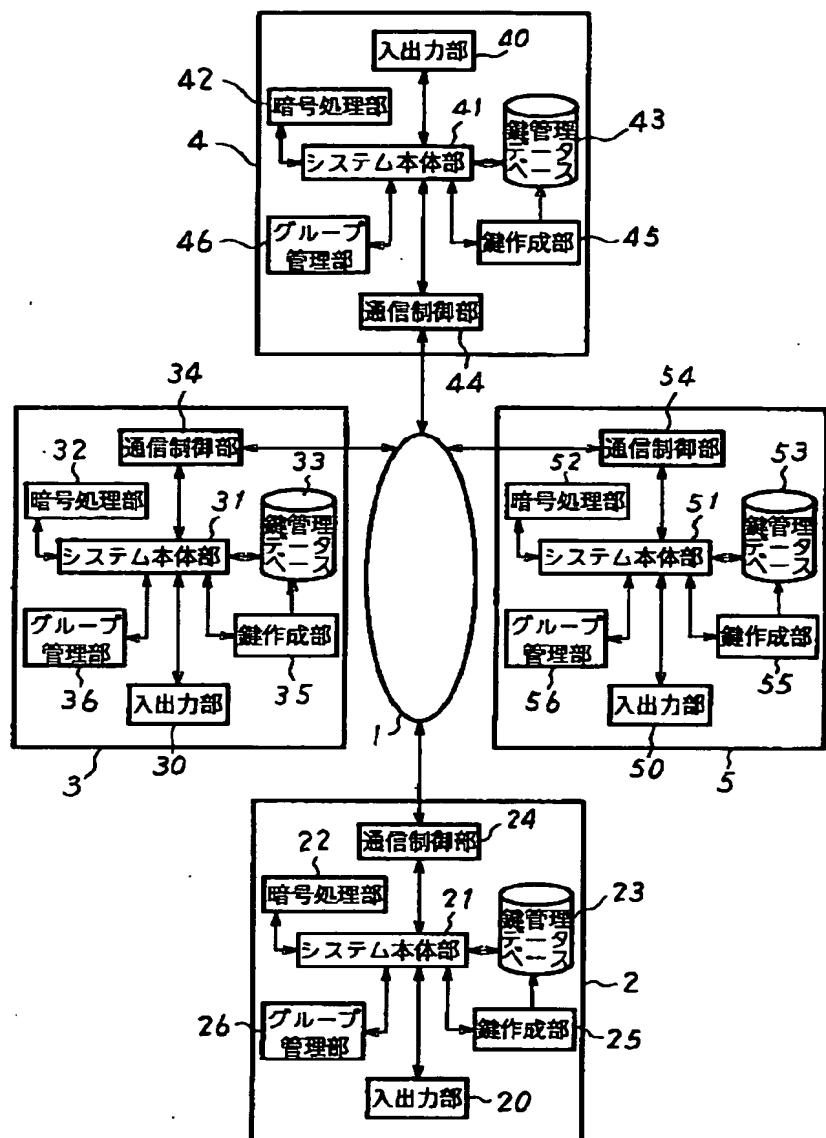
【図3】



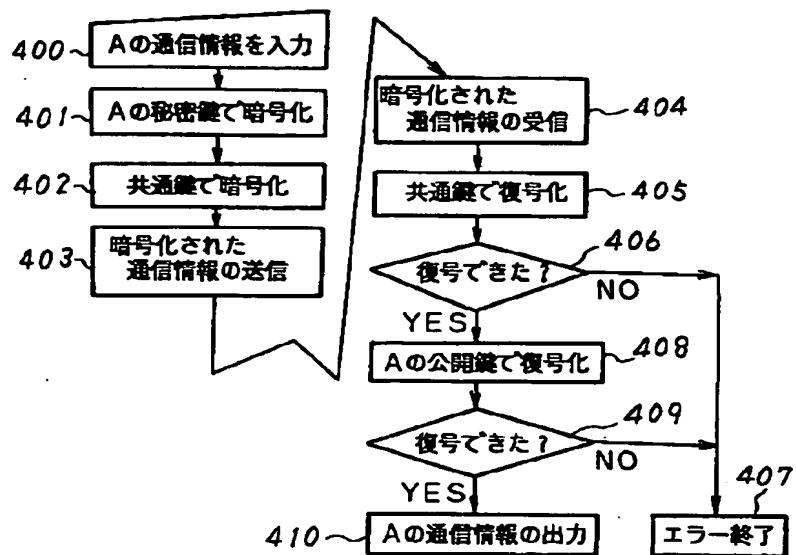
【図5】



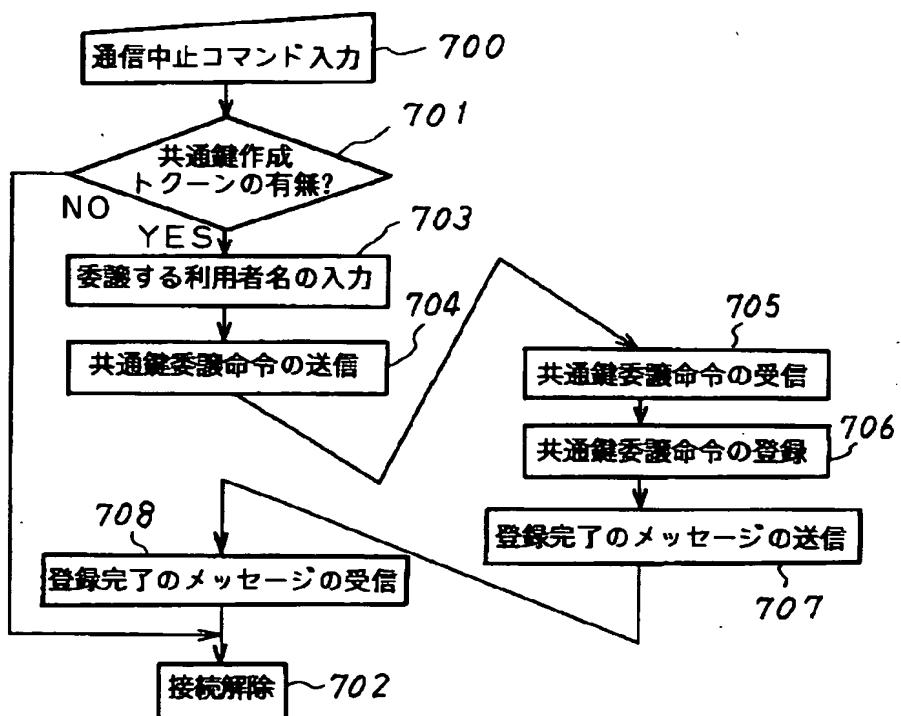
【 図1 】



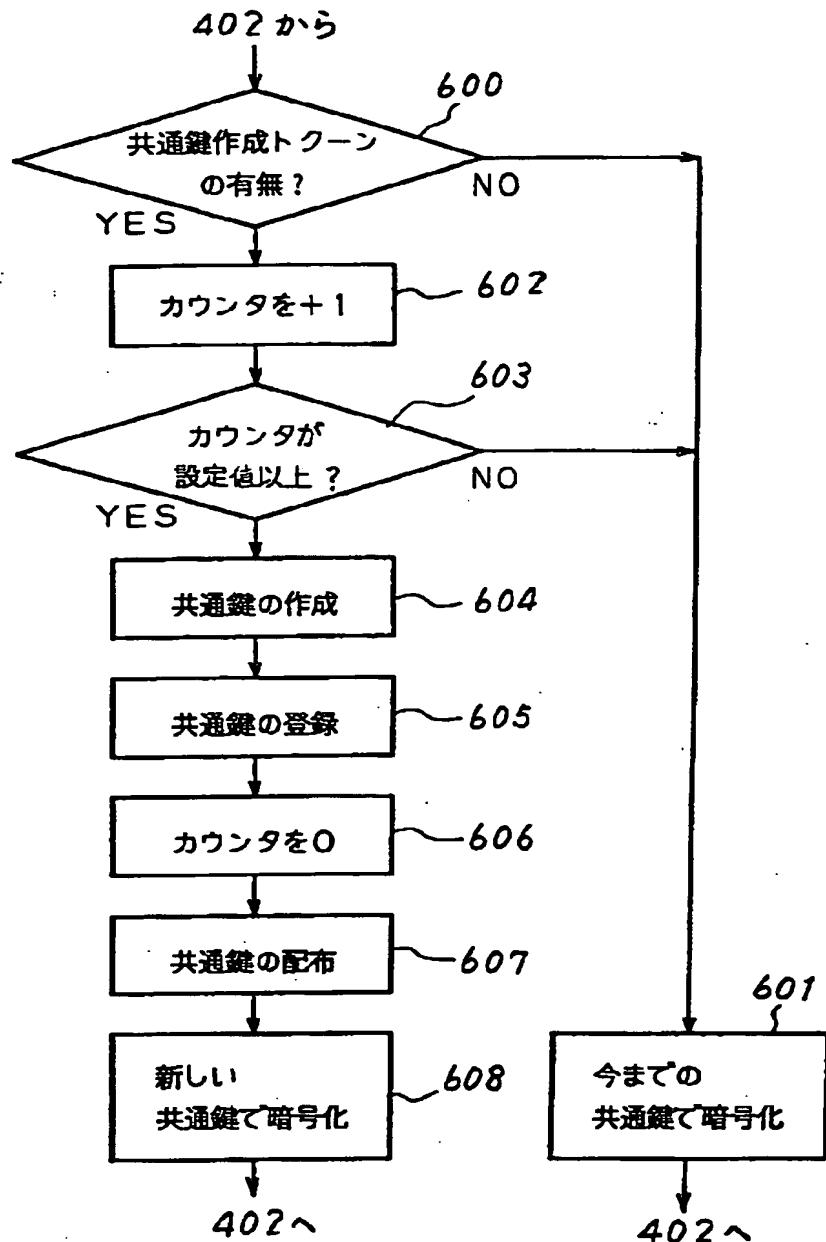
【 図4 】



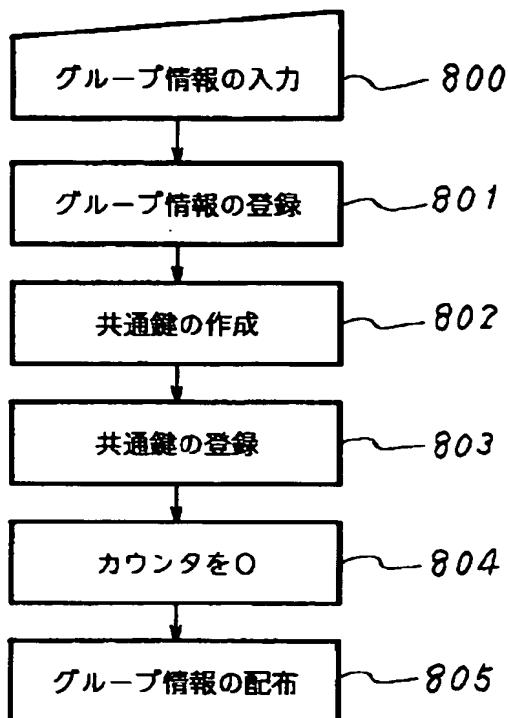
【 図7 】



【 図6 】

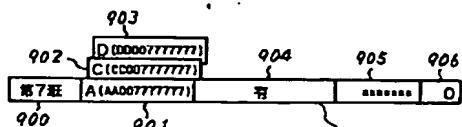


【 図8 】



【 図9 】

グループ名	利用者情報リスト	新作成トクーンの有無	共通鍵	カウンタ




フロント ページの続き

(51) Int.CI.<sup>5</sup>

G 0 6 F 13/00  
 H 0 4 L 9/06  
 9/14  
 12/22

識別記号 庁内整理番号

3 5 1 Z 7368-5B

F I

技術表示箇所

8732-5K

H 0 4 L 11/26